UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

THE PEOPLE OF THE STATE OF NEW YORK, by LETITIA JAMES, Attorney General of the State of New York, Plaintiff, v. CITIBANK N.A., Defendant.	Case No. 24 Civ. 0659

MEMORANDUM OF LAW IN OPPOSITION TO THE MOTION TO DISMISS OF DEFENDANT CITIBANK N.A.

LETITIA JAMES
Attorney General of the
State of New York

Christopher L. Filburn
Assistant Attorney General
Bureau of Consumer Frauds & Protection
28 Liberty Street, 20th Floor
New York, New York 10005
212.416.8303

Counsel for Plaintiff People of the State of New York, by Letitia James, Attorney General of the State of New York

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

RULES & REGULATIONS

OTHER AUTHORITIES

INTRODUCTION

This lawsuit seeks to hold Citibank N.A. ("Citi") to account for its improper exposure of countless consumers to the theft of their life savings, kids' college funds, and retirement nest eggs, its failure to follow the law by investigating and correcting errors, and its deceptive handling of consumers' claims of fraudulent account activity. Citi's motion to dismiss repeatedly attacks the Complaint for a new and unprecedented application of federal law. But Citi inverts reality. There is nothing new about banks being strictly liable for unauthorized transfers from consumer bank accounts that are initiated anonymously and electronically at ATMs, with debit cards, or through online and mobile banking. That liability is the bedrock of electronic banking in the United States. What is new is that Citi recently provided consumers, for the first time, the power to request that Citi send tens of thousands of dollars on their behalf, in instant and irrevocable wire transfers, and to authorize Citi to transfer funds from their bank accounts to pay for such services. But Citi's calamitous rollout of these services lacked the basic hallmarks of security for electronic banking, exposing consumers to sophisticated scams that have cost them everything in their accounts—with no knowledge whatsoever that a single cent was ever at risk. This lawsuit seeks to rectify these wrongs, to restore consumer confidence in online and mobile banking, and to apply the law in the manner that has successfully fostered electronic payments for more than four decades.

The Electronic Funds Transfer Act (the "EFTA") is the foundation on which electronic banking is built the United States. Its centerpiece is a strict liability regime for unauthorized or erroneous electronic fund transfers, referred to as "EFTs," such as ATM withdrawals, debit card purchases, and online transactions. Its goal is to prevent disaster: "A consumer could awake one morning and find that his or her entire savings has disappeared by virtue of a surreptitious computer manipulation," the law's sponsor explained. To incentivize banks to make electronic banking reliable, the EFTA requires them to correct errors and reimburse unauthorized EFTs.

Faced with the prospect of limitless liability, banks took action to protect themselves (and, as a result, to protect consumers.) The EFTA is why daily ATM limits exist. The EFTA is why calls regarding suspicious debit card transactions exist. The EFTA is why text messages to confirm $100 Zelle transfers exist. The tradeoff is straightforward and fundamental to electronic banking: banks put in guardrails to limit their own potential losses from unauthorized EFTs, some of which consumers might find annoying from time to time, but in exchange consumers are assured that their money is safe and that they will get it back if errors or unauthorized activity occurs.

As alleged, Citi recently connected consumers' online and mobile banking to wire network services traditionally used by banks and businesses to move trillions of dollars all around the world. As a result, consumers no longer need to go to a local branch to ask Citi to wire money—a rare event for most that might occur once or twice, such as to buy a home. Instead, with a username, a password, and a few clicks, consumers can request that Citi send tens of thousands of dollars on their behalf and authorize EFTs from their accounts to pay Citi for this service.

But so too could scammers who infiltrate online or mobile banking. Yet in rolling out this new EFT system, Citi inexplicably omitted the guardrails. No daily or transaction limits. No in-person verification or direct-contact protocols. And no sophisticated monitoring of anomalous activity: In minutes scammers change passwords, upgrade accounts, enroll in wire services, move money, and send thousands of dollars to unknown persons—with minimal verification.

Citi's omissions exposed consumers to the very risk of total loss that the EFTA sought to eliminate. And the results have been the stuff of nightmares. One consumer was at work when she noticed her mobile phone stopped working (Complaint, ECF No. 1, at ¶ 170 (hereinafter, "¶¶ __")); she checked her email a few hours later and found that $50,000 had been removed from her bank account, all without a word from Citi (¶¶ 168–81). Another consumer attempting to log in to online

banking received an alert that her account was suspended, so she called the provided number and worked with a Citi representative to secure her account (¶¶ 218–19); the next day she discovered $35,000 was gone, leaving her with little money in the bank and forcing her to turn to expensive loans to get by (¶¶ 217–31). A third consumer who banked with Citi received a text message asking about a $7,750 wire transfer and pressed "3" to say he didn't recognize the activity (¶ 185); after waiting on hold for nearly an hour, he was told that he had less than $75 left (¶¶ 182–96).

The EFTA should have saved these consumers and many more who have lost millions in sophisticated scams during which they had no idea that any money was at risk. Yet having failed to implement commonsense security and exposed consumers to risks of total loss, Citi instead looked to save itself. As alleged, Citi systematically exploited a narrow exemption for interbank transactions, Citi's representatives pushed consumers to execute unnecessary affidavits describing the scams they fell for, and Citi used this information to summarily deny reimbursement.

First, Citi repeatedly and illegally failed to properly investigate, provisionally credit, and repay consumers for unauthorized EFTs initiated by scammers to pay for wire transfers (Count I), failed to reimburse consumers for unauthorized EFTs that consolidated money into one bank account to facilitate scammers' larger-dollar wire transfers (Count II), and imposed adhesive contract terms that undermined consumers' rights under the EFTA (Count III).

Citi's motion to dismiss invites the Court to inhabit an alternate reality in which Citi has linked online and mobile banking to wire network services for eons and regulators and courts have for decades said that the EFTA does not apply. But there is not a single statement identified by Citi in which a court, a regulator, or any authority declared that consumer EFTs that pay for wire services are exempt. Rather, Citi made the decision to offer a novel product and then rely on an expansive reading of a narrow, decades-old exception to insulate itself from liability. The EFTA,

however, exempts ***only*** transfers ***by banks on behalf of consumers over the wire networks***—it says nothing about consumer EFTs. Citi's arguments that this narrow exemption sweeps more broadly cannot be squared with the EFTA's text, its structure, or its purpose.

Second, even under the Uniform Commercial Code ("UCC") that Citi urges the Court to apply, Citi repeatedly and illegally failed to repay consumers for fraudulent wire requests that were not legally effective because (i) Citi's security procedures were not commercially reasonable and (ii) the Complaint alleges detailed facts showing that Citi failed to follow its procedures, did not act in good faith, and did not adhere to consumers' instructions. (Count IV.) Citi ignores the extensive allegations about its own procedures and actions, and instead asks the Court to adopt an inadequate test for commercial reasonableness that is not up to industry standards.

Third, Citi repeatedly and illegally failed to develop and implement technical safeguards to protect consumer financial account information and inadequately trained personnel to respond effectively to consumer account breaches, in violation of New York's SHIELD Act (Count V), and Citi implemented security protocols that failed to identify potential identity theft or respond in a manner that mitigated harm, in violation of the Red Flag Rule (Count VI). Citi's arguments to the contrary fail to engage with the facts and consumer experiences pled in the Complaint and instead push an overbroad preemption theory that is unsupported by law or precedent.

Finally, Citi repeatedly engaged in fraudulent and deceptive business practices by misleading consumers about their EFTA rights, deceiving them into providing sworn evidence that Citi then used to deny their claims under the UCC, making unkept promises about the security of funds in accounts or the likelihood of recovering stolen funds, and falsely promising around-the-clock, effective security for consumer accounts. Citi's motion to dismiss fails to address the factual allegations supporting these claims and does not otherwise provide a basis for dismissal.

BACKGROUND

I. CONGRESS ENACTED THE EFTA TO ENCOURAGE THE GROWTH OF ELECTRONIC BANKING BY PROVIDING KEY CONSUMER PROTECTIONS

Congress enacted the EFTA in 1978 to govern emerging EFT systems, which at the time included ATMs, direct deposits, and debit cards, out of concern that these new technologies lacked the protections of in-person banking or signatures and were "vulnerable to fraud" or "unauthorized use." (H.R. Rep. 95-1315, at 2; *see also* S. Rep. 95-915, at 5 (the "face-to-face contact involved in passing a forged check or using a stolen credit card does not act as a deterrent in the EFT context").) Congress also worried that consumers were unaware "of the risk of losing their life savings." (H.R. Rep. 95-1315, at 2.) The law's sponsor warned: "A consumer could awake one morning and find that his or her entire savings has disappeared by virtue of a surreptitious computer manipulation." (Declaration of Christopher L. Filburn ("Filburn Decl.") Ex. A, at 27940 (123 Cong. Rec. 27940); *see id*. Ex. B, at 37011 (123 Cong. Rec. 37009) ("The consumer could lose everything.").)

These same risks threatened to stunt growth; before consumers would "give up known and reliable payment systems" they would "need to be secure in knowing that" their money was safe. (H.R. Rep. 95-1315, at 9; *see* Filburn Decl. Ex. D, at 9116 (124 Cong. Rec. 9116) ("progress toward [EFT] systems" is not possible unless consumers are "assured of . . . safeguards").)

Congress recognized that banks were "in a position to make" EFT systems "secure" (H.R. Rep. 95-1315, at 10), as "the financial institution has established the EFT system and has the ability to tighten its security characteristics" (S. Rep. 95-915, at 6). Yet Congress understood that if consumers are "held responsible for any losses" then banks would "have no incentive to improve [their] security measures." (Filburn Decl. Ex. B, at 37012 (123 Cong. Rec. 37009).) Congress enacted the EFTA to protect consumers and ensure "the financial institution has an incentive to provide a secure EFT system." (S. Rep. 95-1315, at 6; *see also* H.R. Rep. 95-1315, at 10.)

To accomplish its aims, the EFTA "provides ***certainty against total loss*** to the consumer." (S. Rep. 95-915, at 6 (emphasis added).) This was done over the objections of the banking industry, which pushed a bill that would have imposed consumer liability for negligence, (Filburn Decl. Ex. F, at § 7(a) (S. 2470)), and a national commission, (*see* S. Rep. 95-915, at 22 ("[The] bill in very few respects follows the recommendations of the Commission.")). The "negligence approach was rejected." (*Id*. at 6; *see* H.R. Rep. 95.1315, at 9 ("If a negligence standard is adopted, as opponents of this legislation have urged, [EFTs] will likely result in many personal tragedies.").)

Congress also recognized that EFT systems in 1978 were "precursors to more sophisticated payment systems." (Filburn Decl. Ex. A, at 27940 (123 Cong. Rec. 27940).) Thus, EFTs were broadly and flexibly defined as "any transfer of funds" that is "initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape." 15 U.S.C. § 1693a(7).

The EFTA's centerpiece is its protection against unauthorized EFTs, which are EFTs (i) "initiated by a person other than the consumer without actual authority" and (ii) "from which the consumer receives no benefit." 15 U.S.C. § 1693a(12). A consumer need only notify her bank of her belief that an unauthorized EFT occurred, *id*. § 1693f(a), which can be done orally or in writing, 12 C.F.R. § 1005.11(b). The statute then requires the bank to investigate and, if an error is found, to quickly correct it. 15 U.S.C. § 1693f(a)–(b). Where banks need more than ten business days to investigate, they must provisionally credit accounts with funds consumers can immediately use. *Id*. § 1693f(c). After investigation, the EFTA provides a three-tiered limit on liability:

- Two-Day Notice: If a consumer provides notice within two business days, her losses are capped at the smaller of $50 or the amount of the unauthorized EFT.
- Sixty-Day Notice: If a consumer provides notice within sixty business days, her losses are capped at the smaller of $500 or the amount of the unauthorized EFT, but only if the bank proves that the losses would not have occurred had the consumer provided notice within two business days.

- Post-Sixty-Day Notice: If a consumer does not provide notice within sixty business days, there is no cap on her losses, but only if the bank proves that the losses would not have occurred had the consumer provided notice within sixty business days.

Id. § 1693g(a). Thus, the EFTA effectively shifts the risk of loss in connection with unauthorized EFTs from consumers to banks. (¶ 43.) Congress believed that this liability-shifting approach that capped consumer losses for unauthorized EFTs reflected "an appropriate and fair sharing of risks between account holders and financial institutions." (H.R. Rep. 95-1315, at 11.)

II. CONGRESS EXEMPTED FROM EFTA COVERAGE INTER-INSTITUTIONAL PAYMENT NETWORKS THAT CONSUMERS COULD NOT ACCESS

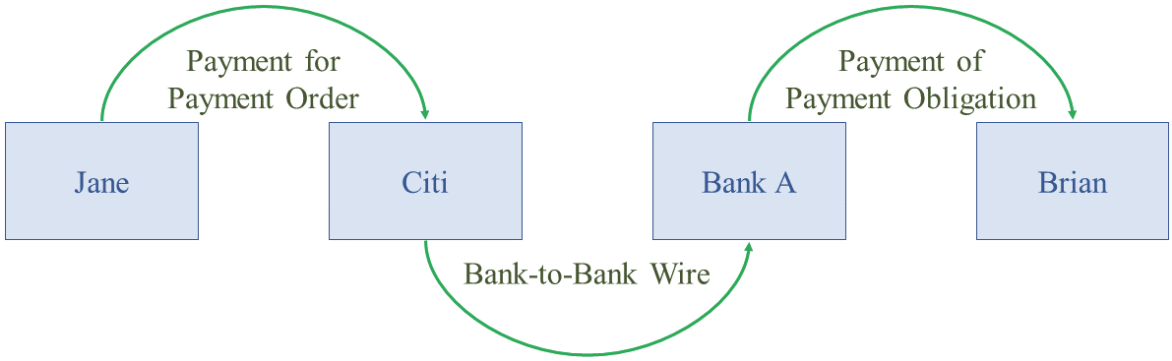
The EFTA addresses the risk of unauthorized EFTs created by increasing consumer "access to electronic fund transfer systems," which in 1978 was "as close as the telephone," (Filburn Decl. Ex. E, at 25735 (124 Cong. Rec. 25730)), and is even more so today. The definition of EFT thus applies to transfers initiated "through an electronic terminal, telephonic instrument, or computer or magnetic tape," 15 U.S.C. § 1693a(7), which are referred to in regulations as "access devices" such as cards, codes, or other means of accessing accounts, 12 C.F.R. § 1005.2(a)(1). Through these definitions, the EFTA covers "only terminals to which the customers of a financial institution have some form of direct access." (Filburn Decl. Ex. C, at 37235 (123 Cong. Rec. 37233).)

Congress also recognized the risks of disrupting services, such as check guarantee services that merchants relied upon or wire networks that banks used to settle their accounts, that might affect consumers, but to which consumers had no direct electronic access. In 1978 and for decades that followed, consumers could request that banks send wire transfers by visiting local branches or submitting signed requests. (¶¶ 23, 26, 29, 45.) To eliminate the risk that this inter-institutional network would be subject to the EFTA simply because consumers might be involved, Congress adopted a narrow exemption for transfers of funds "by means of a service that transfers funds held at either Federal Reserve banks or other depository institutions"—*i.e.*, funds sent over the wire

networks—even when made "on behalf of a consumer." 15 U.S.C. § 1693a(7)(B). Congress explained that this excluded from coverage "traditional 'wire' transfers between banks." (S. Rep. 95-915, at 4, 8; *see* Filburn Decl. Ex. C, at 37233 (the EFTA "would not apply to purely inter-institutional networks such as the Bank Wire or Fed Wire") (123 Cong. 37233).)

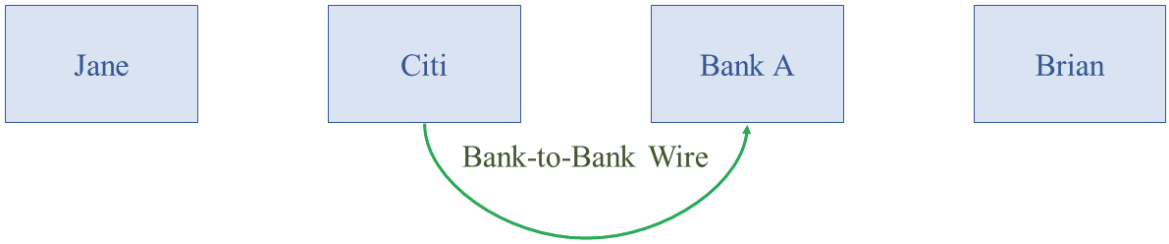
III. ARTICLE 4A OF THE UCC GOVERNS NON-CONSUMER EFTS, SUCH AS BANK-TO-BANK TRANSACTIONS, BUT EXPRESSLY DEFERS TO THE EFTA

The act of "wiring" money—say, from Jane to Brian—is a unique, multi-faceted process. (¶ 58.) It begins when Jane submits a request to Citi, called a "Payment Order," instructing Citi to cause another bank, say Bank A, to pay Brian. (¶¶ 47–48.) In exchange, Jane promises to pay Citi. (¶ 54.) If it accepts Jane's Payment Order, Citi will send a new Payment Order to Bank A over a wire network, such as Fedwire or CHIPS, instructing Bank A to pay Brian. (¶¶ 49–53.) The Payment Order from Citi to Bank A is referred to in the Complaint and herein as a "Bank-to-Bank Wire." If Bank A accepts Citi's Payment Order, Bank A becomes indebted to Brian. (¶ 54.) The result is that money has moved from Citi to Bank A in the Bank-to-Bank Wire, while Jane has become obligated to pay Citi and Bank A has become obligated to pay Brian (¶ 54):



Today's wire networks, Fedwire and CHIPS, began as electronic means for banks to settle their accounts, (¶ 44), before growing commercially (¶ 45). As wiring money became a common form of commercial payment, UCC Article 4A was adopted to provide a legal framework for the networks. U.C.C. art. 4A, Official Comment, Prefatory Note (hereinafter "UCC Pref. Note").

Article 4A defines a Payment Order as an instruction "to pay, or to cause another bank to pay," a beneficiary. U.C.C. § 4A-103(1)(a)(ii). And it defines a "funds transfer" as the "series of transactions beginning" with the initial Payment Order that "is completed by acceptance by the beneficiary's bank of a payment order." U.C.C. § 4A-104(1). While the UCC follows the "convention" of using "funds transfer" to refer to the payment from Jane to Brian, in fact "***no money or property right of [Jane] is actually transferred to [Brian]***." UCC Pref. Note (emphasis added). Instead, Citi ***sends its own money*** in a Bank-to-Bank Wire and then is "reimbursed by debiting [Jane]'s account or otherwise receiving payment from" her. U.C.C. § 4A-104(1)(a)(ii). "The effect" of these definitions is to "limit article 4A to payments made through the banking system," *id*. § 4A-104, Official Comment, as illustrated in the Complaint (¶ 53):



The UCC requires banks to reimburse payments for unauthorized Payment Orders, with interest. U.C.C. § 4A-204(1). Banks can avoid these obligations only if an unauthorized Payment Order was "effective," which requires that: (i) an agreed-upon "security procedure" that "is commercially reasonable" was in place; and (ii) the bank "proves" that it accepted the Payment Order in good faith, in compliance with the security procedure, and in compliance with customer instructions. *Id*. §§ 4A-202(2), 4A-204(1). Security procedures are negotiated between banks and their customers. *See id*. § 4A-201 (procedures must be "established by agreement").

Whether a particular security procedure is commercially reasonable is a question of law. *Id*. § 4A-202(3). Courts determine whether a particular security procedure was commercially reasonably by evaluating several factors specified by Article 4A, including "the wishes of the

customer" and the "circumstances of the customer known to the bank." *Id*. § 4A-202(3). Thus, "whatever knowledge the bank does have about the customer is relevant in determining the commercial reasonableness of the security procedure." *Id*. § 203, Official Comment.

Article 4A governs transactions typically involving "sophisticated businesses or financial organizations," UCC Pref. Note, and expressly provides that it "does not apply to a funds transfer any part of which is governed" by the EFTA, U.C.C. § 4A-108(1). Moreover, the UCC specifies that "in the event of an inconsistency" between Article 4A and EFTA provisions, the EFTA provisions govern. *Id*. § 108(3); *see id*. § 4A-108, Official Comment ("[I]f a funds transfer is to a consumer account in the beneficiary's bank and the funds transfer is made in part by use of Fedwire and in part by means of an automated clearing house, EFTA applies to the ACH.").

Federal regulators thus have explained that if a bank "makes a fund transfer to a consumer's account after receiving funds through Fedwire," the ACH transfer is subject to the EFTA "though the Fedwire . . . is exempt." 12 C.F.R. § 1005.3(c)(3), Supp. I, Comment 3(c)(3); *see* 55 Fed. Reg. 40791, 40804 (Oct. 5, 1990) (Federal Reserve: a "funds transfer from a consumer originator or a funds transfer to a consumer beneficiary could be carried out in part through Fedwire and in part through an [ACH] or other means that is subject to the" EFTA). Indeed, the Federal Reserve recognized that the UCC's deference to the EFTA in such cases could leave "the rights and obligations of the Federal Reserve Banks and their direct senders and receiving banks" less than "fully defined" because Section 4A-108 would take the entire funds transfer out of Article 4A. *Id*. at 40799. It thus promulgated Subpart B of Reg. J, which "applies to any party to a Fedwire transfer that is in privity with a Federal Reserve Bank," *id*. at 40803; 12 C.F.R. § 210.25(b)(2)(i)–(iii), and which incorporates Article 4A to "govern funds transfers through the Fedwire Funds Service" for these parties, 12 C.F.R. § 210.25(a), even where a consumer EFT is part of the process.

IV. CITI'S PROVISION TO CONSUMERS OF ELECTRONIC ACCESS TO WIRE NETWORK SERVICES COST CONSUMERS MILLIONS OF DOLLARS IN UNAUTHORIZED EFTS THAT CITI DID NOT PREVENT OR REIMBURSE

A. Citi Offered Online and Mobile Banking Platforms to Consumers that Included Direct Electronic Access to Wire Network Services

As the rise in widespread internet access and mobile device use has driven most adults to primarily bank electronically (¶¶ 24–25), Citi aggressively pushed this transition by promoting a safe and secure electronic banking experience (¶¶ 79–83). Citi promised "24/7 fraud detection services and security features" (¶ 82) and described security as its "topmost priority" (¶ 83).

When enrolling in electronic banking, consumers must agree to Citi's online terms and conditions and its agreement for online fund transfers (¶¶ 11, 56, 84), a process involving no negotiation (¶¶ 8, 85–87). The terms and conditions supplant Citi's client manual, its standard banking agreement that consumers agree to when opening bank accounts with Citi, which contains a security procedure that requires Citi to call consumers to verify Payment Orders. (¶¶ 77–78.) Instead, the terms and conditions state that use of an online username and password is sufficient to verify Payment Orders (¶¶ 84–85, 88–89), and provide that Citi's records will be "conclusive" evidence of authorization (¶ 89). The revised procedures also state that Citi "may" employ other verification tools. (¶ 84.) Finally, the agreements provide that requests for transfers through online or mobile banking act as authorizations for Citi to debit consumer accounts. (¶ 56.)

For many years, consumers who enrolled in online or mobile banking would still need to travel to local Citi branches to access wire transfer services (¶¶ 23, 26, 44–45, 55), and consumer wire use remained a small proportion of all wire transfer activity (¶¶ 23, 27–28). In recent years, however, Citi provided its online and mobile banking users with direct electronic access to these services. (¶¶ 5, 26, 29, 56.) As a result, for the first time, consumers who bank with Citi could electronically submit a Payment Order and authorize EFTs to pay for the service. (¶ 58.)

B. Citi's Woefully Inept Security Protocols Enabled the Theft of Millions of Dollars from Consumers by Scammers Who Accessed the Wire Networks

Citi's provision of electronic access to wire services exposed consumers to sophisticated scams that weaponize Citi's systems against them. (¶¶ 29–32.) Phishing scams in which scammers try to trick consumers into sharing personal or account information have exploded. (¶¶ 30–31.) For example, consumers received phone calls that displayed "Citibank" with a number matching Citi customer service (¶¶ 140, 236, 249), and well-trained scammers impersonating Citi were on the other end. Similarly, consumers attempting to log in to online banking received alerts that accounts were locked and were provided a number to contact Citi. (*E.g.*, ¶ 218.) And SIM swaps, through which scammers took over mobile devices to impersonate consumers and reset banking apps, have been a constant threat. (¶¶ 32, 170–72, 199–205.) Citi did not respond effectively to defeat scams that utilized its own website, phone number, and text-verification tools. (¶¶ 35–36.)

Having exposed consumers to these threats, Citi's verification protocols utterly failed. For example, Consumers B, E, and I had never used wire transfer services before but had their accounts drained, losing $22,000, $50,000, and $15,000, without any direct contact from Citi. (¶¶ 103–06, 139–52, 168–81, 232–47.) When scammers suspiciously consolidated consumers' funds from multiple accounts in a well-known effort to avoid scrutiny, Citi did not strengthen its verification processes. (¶¶ 94, 103, 277–78.) For example, Consumer C's accounts had $1,887, $4,000, and $10,000 transferred into a single account with a resulting balance of 38,763.27 just before Citi accepted a $37,700 Payment Order and debited his account, leaving less than $1,000. (¶¶ 155–56.) Nine thousand dollars was transferred from Consumer G's savings account to his checking account, creating a balance just over $27,000, before Citi accepted a $27,000 Payment Order and debited his account. (¶¶ 199, 205.) And Consumer H's accounts had $3,544.18, $5,169.19, and $6,091.44 transferred into a single account with a resulting balance of $36,031 just before Citi

accepted a $35,000 Payment Order and debited her account. (¶¶ 221–25.) In none of these cases did Citi attempt to verify—or even provide notice of—the unauthorized transfer activity. (¶¶ 62, 94, 155, 199, 220.) Nor did Citi apply more robust verification procedures to the large-dollar, account-emptying Payment Orders that immediately followed. (¶¶ 103, 105.)

Citi's alternatives to direct-contact verification have not effectively identified or defeated fraudulent activity. (¶ 90.) Despite awareness of the threat posed by SIM swaps (¶ 36), Citi relied on text verification of suspicious activity, sending the text messages directly to scammers. (¶¶ 170–72, 201.) Citi also sent text messages instructing consumers to contact Citi, but then consumers faced extensive hold times while scammers completed their scams. (¶¶ 108, 111, 185, 238–39.) When scammers were unable to satisfy verification protocols and Citi rejected Payment Orders, Citi applied alternative verification protocols permitting scammers to complete identical Payment Orders moments later. (¶¶ 104, 126–28, 203–05, 250–53.) And Citi permitted scammers to contact it directly to override verification protocols. (¶¶ 108, 111, 143–44, 186, 239.)

Citi likewise failed to respond appropriately to obvious red flags of fraudulent infiltration of online or mobile banking, such as changes to usernames, passwords, or account status, by subjecting large-dollar Payment Orders to robust scrutiny (¶¶ 12(a), 100–02, 105). For example:

- Consumer A: Her online password was changed, her account was enrolled in online wire transfer services, and a $39,999 wire transfer was attempted but failed, all before Citi accepted a fraudulent $40,000 Payment Order and debited that amount, plus a $17.50 fee, from her account. (¶¶ 123–38.)

- Consumer E: Despite having never sent a wire in more than 20 years with Citi, her account status was upgraded and enrolled in online wire transfer services, all before Citi accepted a $50,000 Payment Order and debited that amount from her account, leaving a balance near $0. (¶¶ 168–81.)

- Consumer F: His account status was upgraded and enrolled in online wire transfer services, and then multiple wire transfers totaling more than $200,000 were attempted but failed, all before Citi accepted fraudulent Payment Orders of $75,000 and $27,000. (¶¶ 197–216.)

- Consumer J: Her online username and online password were changed, and three wire transfers in excess of $45,000 were attempted but failed, all before Citi accepted Payment Orders of $9,800, $9,700, $9,900, and $9,897, two of which were accepted by Citi after Consumer J contacted Citi and described her interactions the prior day with a scammer. (¶¶ 248–62.)

Citi's procedures did not require direct contact with these consumers before executing large-dollar transfers initiated shortly after such unusual activity. (¶¶ 100–02, 105, 126, 171, 207, 256.)

Nor did Citi empower consumers to defeat fraudulent activity in real time. (¶¶ 12(c), 107–13.) Consumers were faced with interminable hold times (¶¶ 108–09, 129, 174, 189, 208, 220, 254) and poorly trained representatives who merely put consumers back on hold while scammers completed their frauds (¶¶ 108–11, 115, 129, 141, 174–75, 186–87, 239–40, 256). Consumers B and F both sat on hold, having already pressed buttons on their phones to deny fraudulent activity, when Citi accepted $22,000 and $7,750 Payment Orders and debited their accounts. (¶¶ 141–45, 185–87.) Consumer D was on hold after having told a Citi representative about ongoing fraud, when Citi accepted a $44,440 Payment Order and debited his account. (¶¶ 161–63.) And Consumer I was crying, having been placed on hold after begging not to be, when Citi accepted a fraudulent $15,000 Payment Order and left her account nearly empty. (¶¶ 238–40.) Adding insult to injury, Citi delayed days (¶¶ 174, 213, 226, 242), and even weeks (¶ 148), before attempting recalls.

C. Citi Responded to the Cascade of Consumer Losses by Imposing Illegal Hurdles to Reimbursement and Deceptively Denying Claims under the UCC

Consumers facing total losses who notified Citi often spoke with poorly trained customer service representatives or branch employees who falsely assured them that money was secure or would be returned. (¶¶ 7, 114, 116, 149, 161, 189, 210.) They were instructed to travel to local branches and were told to complete form affidavits. (¶¶ 8, 59–60, 113, 118.) Citi representatives encouraged consumers to include detailed descriptions of events and often filled out the affidavits, ensuring that any details that might suggest consumers inadvertently provided information to

scammers was captured in sworn statements. (¶¶ 9, 61, 164, 177.) And consumers who questioned the affidavits were told that Citi would not investigate or take any action that might result in reimbursement until the affidavits were executed and notarized. (¶¶ 8, 118, 164.)

Nowhere in this process did Citi's representatives or its affidavits refer to consumer EFTs that funded fraudulent Payment Orders or mention the EFTA. (¶¶ 7–8, 62, 60 65, 120, 269–271.) Citi's investigations were perfunctory and, in many cases, did not even include a basic interview (¶¶ 63, 65, 136, 165, 229, 261), nor did Citi provisionally credit accounts as weeks went by (¶¶ 62, 120, 271(b)). Consumers then received form letters stating one of a few predetermined bases for denial (¶¶ 64, 66), such as that they "did not take adequate steps to safeguard" their accounts or fell for "a scam" (¶ 65). Subsequent appeals were summarily denied. (¶¶ 65, 137, 166, 180, 195, 230.) And even in the rare occasions where Citi reimbursed consumers—often only after inquiry by the OAG (¶¶ 167, 196, 216, 262)—Citi did not pay interest (¶¶ 119, 247, 262, 296).

Consumers have lost everything in their accounts, their kids' college savings, and their retirement nest eggs, amounting to millions of dollars. (¶¶ 4, 34, 121.) And the harms only start there: Affected consumers suffer fear, shame, and depression, and frequently are forced to turn to expensive forms of credit to make up shortfalls in their finances. (*E.g.*, ¶ 122.)

STATUTORY FRAMEWORK & LEGAL STANDARD

New York's Executive Law § 63(12) empowers the OAG to seek injunctive and other relief when a person or business engages in repeated or persistent fraudulent or illegal conduct. Illegality includes violations of state or federal law or regulations. *See FTC v. Shkreli*, 581 F. Supp. 3d 579, 627–28 (S.D.N.Y. 2022) (Sherman Act); *State v. Scottish-Am. Ass'n, Inc.*, 52 A.D.2d 528, 528 (N.Y. App. Div. 1976) (Civil Aeronautics Board regs). Conduct is "repeated" if there is "repetition" of any "illegal act or conduct which affects more than one person," while conduct is "persistent" if there is a "continuance or carrying on" of any "illegal act or conduct." N.Y. Exec.

Law. § 63(12). The OAG is not required to establish a particular numerical threshold or significant percentage of violations. *State v. Princess Prestige Co., Inc.*, 42 N.Y.2d 104, 107 (1977).

Claims asserted under the Executive Law are subject to Rule 8 of the Federal Rules of Civil Procedure. *CFPB v. RD Legal Funding, LLC*, 332 F. Supp. 3d 729, 751 (S.D.N.Y. 2018). Rule 8 requires a "short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). A court "must accept the material facts alleged in the complaint as true and construe all reasonable inferences in the plaintiff's favor." *RD Legal*, 332 F. Supp. 3d at 751 (quotations omitted). Dismissal is appropriate only if the alleged facts fail to establish a "plausible" claim for relief. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555–56 (2007). This pleading standard does not require detailed factual allegations but merely notice of facts supporting the elements of the claim. *Hagan v. City of N.Y.*, 39 F. Supp. 3d 481, 494 (S.D.N.Y. 2014) (Oetken, J.).

ARGUMENT

I. THE COMPLAINT ADEQUATELY ALLEGES REPEATED AND PERSISTENT ILLEGALITY BASED ON CITI'S VIOLATIONS OF ITS EFTA AND REG. E OBLIGATIONS TO CONSUMERS FOR UNAUTHORIZED EFTS (COUNT I)

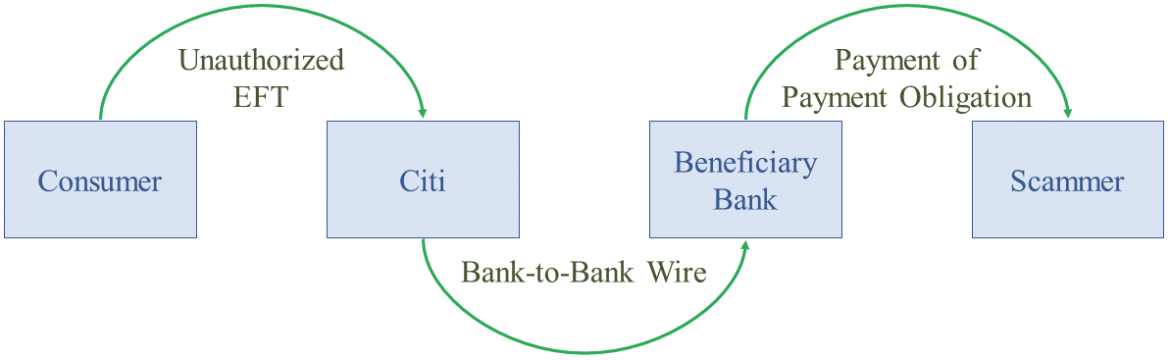
Under the EFTA and Reg. E, Citi must provisionally credit accounts and reimburse losses for unauthorized EFTs. 15 U.S.C. §§ 1693a, 1693f, 1693g; 12 C.F.R. §§ 1005.3, 1005.6, 1005.11. Count I alleges that Citi failed to do so. (¶¶ 267–71.) Citi does not dispute its failure to do so but argues that when scammers infiltrate online or mobile banking to initiate wire transfers the resulting consumer EFTs are part of exempt "consumer wires" (*id*. 13–20). Citi is wrong.

A. The Complaint Adequately Alleges the Existence of Unauthorized EFTs

An EFT is a transfer "initiated through an electronic terminal, telephonic instrument, or computer or magnetic take so as to order, instruct, or authorize a financial institution to debit or credit an account" that includes "but is not limited" to several examples. 15 U.S.C. § 1693a(7). This definition was "left open" because "computer technology was still in a rapid, evolutionary

stage of development." *Spain v. Union Trust*, 674 F. Supp. 1496, 1499 (D. Conn. 1987). Congress thus sought to ensure "that all equivalent EFT systems are subject to the same standards," as "no one can forsee EFT developments in the future." (S. Rep. 95-915, at 3–5, 10).

The Complaint alleges that Citi recently enabled consumers to use online and mobile banking to submit Payment Orders and electronically authorize Citi to debit accounts, which scammers fraudulently accessed to execute unauthorized consumer EFTs, as illustrated:



(¶¶ 56–58.) The Complaint also alleges that consumers did not benefit from these EFTs as the money was removed from their accounts and they did not benefit from the wire transfers. (¶ 270.) The Complaint thus alleges the existence of "unauthorized" EFTs. 15 U.S.C. § 1693a(12).

B. The EFTA's Wire Exemption Does Not Apply to these Unauthorized EFTs

The language of the EFTA, the structure of its definitions, and the purpose that underlies it all point to the same conclusion: the consumer EFTs described above are not exempt.

1. The Plain Language of the Wire Exemption Does Not Reach the Unauthorized EFTs Alleged in the Complaint

"Well-established principles of construction dictate that statutory analysis necessarily begins with the plain meaning of a law's text and, absent ambiguity, will generally end there." *Collazos v. U.S.*, 368 F.3d 190, 196 (2d Cir. 2004). Here, the EFTA exempts a transfer "made ***by a financial institution on behalf of a consumer*** by ***means of a service*** that transfers funds held at either Federal Reserve banks or other depository institutions." 15 U.S.C. § 1693a(7)(B) (emphasis

added). There is no ambiguity: "on behalf of" refers to a party—Citi—acting as a representative or stand-in for consumers. *See* Merriam-Webster Dictionary, online ed. (last accessed Apr. 17, 2024) ("as a representative of"); Black's Law Dictionary (11th ed. 2019) ("on behalf of means 'in the name of, on the part of, as the agent or representative of'"). And "means of a service" refers to services such as Fedwire or CHIPS. Thus, as the Federal Reserve explained when promulgating Reg. E, the exemption covers a "transfer of funds for a consumer" over the wire networks. 44 Fed. Reg. 18468, 18481 (Mar. 28, 1979). That is the Bank-to-Bank Wire. (¶¶ 53–54.)

By contrast, the Complaint alleges that consumer EFTs that pay for fraudulent Payment Orders are made directly from consumers' accounts (¶¶ 56–57, 93, 98), and are not sent over the wire networks (¶¶ 54–58, 269). The EFTA exempts only transfers "by a financial institution" made "by means of a [wire] service," 15 U.S.C. § 1693a(7)(B)—it does not exempt "related payments"; it does not exempt payments "by a consumer"; and it does not exempt payments "from consumer accounts." The EFTs at issue therefore are not exempt. *See Simmons v. Himmelreich*, 578 U.S. 621, 627 (2016) (courts "presume Congress says what it means and means what it says").

2. The EFTA Exempts Inaccessible Payment Networks

Exempting only Bank-to-Bank Wires is consistent with the EFTA's distinction between payment networks to which consumers do or do not have access. Congress was concerned that accessible networks were vulnerable because they lacked the "face-to-face contact" provided by in-person banking. (S. Rep. 95-915, at 5), and thus intended the EFTA to safeguard "terminals to which the customers of a financial institution have some form of direct access." (Filburn Decl. Ex. C, at 37235 (123 Cong. Rec. 37233).) As a result, the EFTA safeguards against unauthorized EFTs made using access devices. 15 U.S.C. § 1693a(1); 12 C.F.R. § 1005.2(a)(1).

Broadly applying the definition of EFT is consistent with ensuring "that all equivalent EFT services are subject to the same standards" as new systems are developed. (S. Rep. 95-915, at 4.)

In 1978, a consumer could use an ATM to electronically authorize Citi to debit her account in exchange for providing cash. Now that Citi connects online and mobile banking to wire services, a consumer can electronically authorize Citi to debit her account in exchange for executing a Payment Order. (¶¶ 5, 56–57.) There is no conceptual difference between these two EFT systems, which are mechanisms to electronically authorize payment for services—whether the provision of cash or the execution of a Payment Order. The language of the EFTA treats them the same.

By contrast, consumers cannot send money directly from their bank accounts over the wire networks; they can only ask Citi to send its own money for them, in exchange for their promise to repay. (¶¶ 5, 23, 26, 51–53.) Accordingly, the EFTA exempts only a transfer "by a financial institution on behalf a consumer by means of a [wire] service," 15 U.S.C. § 1693a(7)(B)."

For this reason, the supposedly apocalyptic policy concerns of Citi's amici are overstated. Applying the EFTA to EFTs that pay for Payment Orders will not impact the wire networks or the relationships among participating banks, which are subject to Subpart B of Reg. J, Article 4A, and CHIPS rules. The sole impact will be that banks who enable consumers to electronically access wire network services will face liability under the EFTA for unauthorized activity, thereby incentivizing them to employ appropriate tools to limit their own liability. But these are tools that ***already exist*** and are ***widely used*** for existing EFT systems through which consumers can directly send money that often serve as substitutes for the transactions here, such as Zelle or ACH networks. Deploying existing safeguards to limit banks' front-end liability would hardly upend the predictability of wire networks—and it is the precise policy choice that Congress already made by broadly defining EFTs and narrowly exempting only Bank-to-Bank Wires.

Nor is there any inconsistency between this narrow exemption and the EFTA's disclosure provisions, as Citi argues (Mot. 19). For one, the exempted transaction is the Bank-to-Bank Wire

and thus doesn't belong on an account statement at all. When the EFTA was enacted, consumers had to travel to branches to execute wire transfers, ensuring that records, such as teller receipts or check slips, would exist. There also is nothing absurd about a line item on a statement today that might identify a "debit by Citi in connection with payment order or wire transfer" for wire transfers executed through online or mobile banking. Guidance already contemplates that statements will "show the institution as the recipient" in certain transactions, such as ATM deposits. 12 C.F.R. § 1005.9, Supp. I, Comment 9(b)(1)(v)-4. And surely such a line item would be sufficient for consumers to "look for errors," as intended. (H.R. Rep. No. 95-1315, at 8.)

3. Congress Adopted the Wire Exemption to Preserve the Functioning of the Wire Networks Not to Exclude a Class of Consumer Transactions

The wire exemption narrowly insulates wire networks dependent on speed and certainty to function (¶¶ 51–53) from disruptions that would be caused by a liability-shifting regime.

Citi argues that because EFTs are defined as transfers to or from consumer accounts and Bank-to-Bank Wires involve only non-consumers accounts, the exemption cannot be read to apply only to Bank-to-Bank Wires under rules of interpretation that disfavor redundant or superfluous statutory language. (Mot. 14.) The Second Circuit, however, has cautioned that such general rules "should not take precedence" if "there are substantial reasons to believe the legislature intended" a particular result. *Hakala v. Deutsche Bank AG*, 343 F.3d 111, 116 (2d Cir. 2003).

Here, there is such clear evidence in two forms. *First*, the statutory language applies only to transfers ***by banks*** (*see supra* Section I.A.1)—it says nothing about consumer EFTs. *Second*, it is indisputable that Congress knew it was exempting transfers that did not involve consumer accounts but did so anyway, as the Senate Report states that "traditional 'wire' transfers ***between banks***" are exempt. (S. Rep. 95-915, at 4, 8; *see also* Filburn Decl. Ex. C, at 37233 (the EFTA "would not apply to ***purely inter-institutional networks*** such as the Bank Wire or Fed Wire") (123

Cong. Rec. 37233) (emphasis added throughout).) Such "evidence of congressional intent can overcome the force of an interpretive canon." *Alliance for Open Society Int'l., Inc. v. USAID*, 430 F. Supp. 2d 222, 247 (S.D.N.Y. 2006). By contrast, there is nothing whatsoever to suggest that Congress—intending to protect consumers from risks inherent in anonymous electronic banking—also intended to carve out an entire class of consumer EFTs from any such protections.

The EFTA's exemptions reflect Congress's exclusion of certain "banking services" from coverage. (S. Rep. 95-915, at 4.) For decades (and today), the wire exemption provided banks an assurance: that a consumer might act as a sender or a beneficiary and that banks wire money using electronic terminals ***does not mean*** that the EFTA applies to Bank-to-Bank Wires. That this assurance may not be technically necessary does not make it meaningless. *See Krause v. Titleserve, Inc.*, 402 F.3d 119, 127 (2d Cir. 2005) (Congress can adopt repetitive or technically unnecessary language to "clarify the meaning of a statute"); *see also Gutierrez v. Ada*, 528 U.S. 250, 258 (2000) (the "rule against redundancy does not necessarily have the strength to turn a tide of good cause to come out the other way" if the "phrase in question has some clarifying value").

That Congress intended to and in fact did adopt technically redundant exemptions for certain banking services to clarify the scope of the EFTA also is shown by the preceding exemption. Specifically, the EFTA exempts "any check guarantee or authorization service which does not directly result in a debit or credit to a consumer account." 15 U.S.C. § 1693a(7)(A). But a transfer that does not debit or credit a consumer account is, by definition, not an EFT and thus is not subject to the EFTA at all, *id*. § 1693a(7)—even without the exemption. Yet in both the check guarantee exemption and the wire exemption Congress identified banking services—check guarantee services for merchants who accept checks and wire services for banks that use them to settle accounts—and adopted narrow, specific exemptions to provide certainty that those services

would not be disrupted by the new law. *See Mellouli v. Lynch*, 575 U.S. 798, 809 ("Statutes should be interpreted 'as a symmetrical and coherent regulatory scheme.'") (citations omitted).

C. Citi's Interpretation of the Wire Exemption to Cover a "Consumer Wire" Is Improper and Inconsistent with the EFTA's Text, Purpose, and History

The Court should reject Citi's argument that fraudulent Payment Orders and unauthorized EFTs comprise "a single wire transfer" that is exempt (Mot. 13), for many reasons:

First, Citi's argument that the OAG artificially deconstructs a wire transfer (Mot. 13) is improper. The Complaint alleges that scammers submit Payment Orders that cause Bank-to-Bank Wires ***and*** authorize EFTs that are ***not*** sent "by Fedwire, CHIPS, or means of any other [wire] service." (¶¶ 47–57, 269–70.) This reflects the unique nature of wire networks, which consumers cannot access directly but must ask their banks to send money over in exchange for promises to repay in separate transfers. (*See supra* 8–9.) The Court thus must assess the effect of the EFTA's wire exemption on each transfer. Citi cannot alter these facts as alleged by force of argument on a motion to dismiss. *Doe v. Columbia Univ.*, 831 F.3d 46, 48 (2d Cir. 2016).

Second, Citi misstates the actual language of the statutory exemption. Citi's motion argues at length that the EFTA exempts "consumer wires." (Mot. 14–15.) But that is not what the EFTA exempts; it exempts transfers "***on behalf of*** a consumer," 15 U.S.C. § 1693a(7)(B) (emphasis added), thereby limiting the exemption to payments made by banks for consumers and not reaching direct consumer EFTs. The term "consumer wire" appears nowhere in either the EFTA or Reg. E. 15 U.S.C. § 1693a(7)(B); 12 C.F.R. § 1005.3(c)(3). Citi's interpretation therefore fails to "conform to the language of the statute" but instead improperly attempts to "add words to the law." *Kidd v. Thomas Reuters Corp.*, 925 F.3d 99, 106 n.9 (2d Cir. 2019) (citations omitted).

Third, Citi's conversion of a narrow exemption for a transfer "on behalf of a consumer by means of a [wire] service," 15 U.S.C. § 1693a(7)(B), into a broad exemption for related payments

cannot be squared with the EFTA's purpose. The EFTA's "primary objective" is "provision of individual consumer rights," 15 U.S.C. § 1693, and thus any proper interpretation must "serve" the "stated purpose of consumer protection." *L.S. v. Webloyalty.com, Inc.*, 954 F.3d 110, 116 (2d Cir. 2020). Congress intended to safeguard against the risks posed by EFT systems' dependency "on computers and the resulting absence of any human contact." *Vigneri v. U.S. Bank N.A.*, 437 F. Supp. 2d 1063, 1066 (D. Neb. 2006). Citi instead would expose consumers to these risks.

Fourth, the UCC does not reflect Citi's "consumer wire" theory. Article 4A clearly states that a sender's payment for execution of a Payment Order is independent of the Bank-to-Bank Wire itself and could be by account debit or other means (*see supra* 8–9)—including, today, by consumer EFT. Consistent with this, the Federal Reserve and the CFPB have issued interpretations explaining that if a portion of a funds transfer is by wire and a portion by ACH, the portion by ACH remains subject to the EFTA. 12 C.F.R. § 1005.3(c)(3), Supp. I, Comment 3(c)(3); 55 Fed. Reg. 40791, 40804 (Oct. 5, 1990). And the Federal Reserve also adopted Subpart B to Reg. J to ensure that Fedwire remains subject to the UCC even if a funds transfer includes a portion that is subject to the EFTA (*see supra* 9–10)—an act that would be entirely superfluous if, as Citi argues, the exemption has always been understood to exclude the entire life of a "consumer wire."

Fifth, Citi's interpretation would not have made sense at enactment as it was not possible for consumers to electronically send Payment Orders to their banks while authorizing payment for wire services by consumer EFTs. *See State v. UPS, Inc.*, 179 F. Supp. 3d 282, 294 (S.D.N.Y. 2016) (interpretations should rely on "factual predicate[s] that Congress understood existed at the time"). In effect, Citi urges the Court to give the exemption a meaning today that would have made no sense in 1978 to avoid a meaning that it believes is redundant. Yet resort to such principles is helpful only if there is "little rational basis to select" among "competing interpretations." *Hakala*,

343 F.3d at 116. That is not the case here for the reasons set forth above, and general principles "should not take precedence over [these] more convincing reasons." *Krause*, 402 F.3d at 128.

Finally, Citi's argument that the exemption reaches all movements of money connected to a wire transfer would enable evasion of liability. Banks could interpose wire transfers into all sorts of electronic banking activity, such as to fulfill consumers' online payment requests or to repay out-of-network ATM operators. Under Citi's expansive interpretation of the exemption, everyday EFTs such as online bill payments or ATM withdrawals that trigger wire transfers would no longer be subject to the EFTA. That is not the purpose of the exemption, and it is not the law.

D. Citi's Selective Quotation of Regulators and Courts Is a Red Herring

The guidance, statements, and precedents cited extensively by Citi (Mot. 15–22) do not support dismissal. The bulk of this material covers a bygone era when it was impossible to electronically initiate Payment Orders and authorize EFTs with online or mobile banking. And the quoted sources are ***entirely silent*** on the treatment of consumers EFTs that pay for Payment Orders. Citi's piecing together of stray commentary to resolve a question that regulators did not purport to face or to answer has no application here should be viewed with skepticism. *Cf. Bd. of Trustees v. Royce*, 238 F.3d 177, 181 n.3 (2d Cir. 2001) (declining to treat language in prior opinion "as a gloss on the regulatory meaning of words and terms that were not at issue" in the case).

For example, Citi highlights the phrase "individual consumers' accounts" in 1981 guidance from the Federal Reserve. (Mot. 15.) But Citi ignores the full phrase: "***instructions for crediting*** individual consumers' accounts." 46 Fed. Reg. 46876, 46879 (Sep. 23, 1981) (emphasis added). That phrase is simply a factual description of a Bank-to-Bank Wire. Moreover, the Federal Reserve in later rulemaking stated in no uncertain terms that transfers "to a consumer beneficiary" could be "in part through Fedwire"— the exempted Bank-to-Bank Wire—and "in part through an [ACH] or other means," in which case the EFTA governs the latter transfer. 55 Fed. Reg. at 40804.

Citi's other regulatory references (Mot. 16–18) are equally inapposite. The FDIC's interpretive letter was issued in 1994 and concerned a sender who "went to her bank in Germany and gave them the equivalent of $200" to be wired to the United States. FDIC, *Users' Rights Under the EFTA in the Event of Bank Error Regarding an Electronic Wire Transfer*, 1994 WL 393720, at *1 (1994). It involved no EFT at all and could never have been subject to the EFTA. And the CFPB's remittance transfer rules merely implemented portions of Dodd-Frank enacted to cover certain wire transfers themselves. 77 Fed. Reg. 6194, 6194 (Feb. 7, 2012). Citi's argument that these rules "would have been unnecessary" were the OAG correct about the wire exemption (Mot. 17) is specious—the OAG is not arguing that "wire remittances" were already covered by the EFTA, as Citi appears to suggest, but that ***consumer EFTs*** that pay for Payment Orders are subject to the EFTA, which is a matter unconnected to and unaddressed by the remittance rules.

Citi next asserts that courts "have recognized" that the EFTA "exempts consumer wire transfers." (Mot. 20.) This is not always the case. *See Regatos v. N. Fork Bank*, 257 F. Supp. 2d 632, 638 n.10 (S.D.N.Y. 2003) ("The EFTA governs wire transfers to and from bank accounts" belonging to consumers); *see also Choice Escrow and Land Title, LLC v. BancorpSouth Bank*, 754 F.3d 611, 616 (8th Cir. 2014) (distinguishing "wholesale wire transfers" under the UCC from "wire transfers by consumers, which are governed by" the EFTA). Indeed, Citi's cases are wholly silent on the question before this Court of whether indisputably ***unauthorized consumer EFTs*** that pay for Payment Orders are subject to the EFTA. Several cases involved no unauthorized EFTs at all but consumers who authorized transfers in person at local bank branches. *See Wright v. Citizen's Bank of East Tennessee*, 640 F. App'x 401, 402 (6th Cir. 2016) (consumer "went to Citizens' branch" to "initiate a wire transfer"); *Pope v. Wells Fargo Bank, N.A.*, No. 23 Civ. 86, 2023 WL 9604555, at *2 (D. Utah Dec. 27, 2023) (consumer "proceeded to drive to her local Wells Fargo

branch" to execute wire transfer); *see also Bodley v. Clark*, No. 11 Civ. 8955, 2012 WL 3042175, at *4 (S.D.N.Y. Jul. 23, 2012) ("plaintiff has not alleged that the purported unauthorized transfer was initiated through an electronic terminal, telephone, computer, or magnetic tape"). Similarly, the decision in *Spain* did not "reject" the argument that a transaction might involve multiple transfers of funds, as Citi's amici suggest (*see* ECF No. 20-1, at 14), but held that the EFTA did not apply because "[b]oth transactions were handled by a bank employee, not an electronic terminal." 674 F. Supp. at 1500. The remaining cases do not support Citi's argument.[1]

Citi finally points to recent hearings before Congress, but its reliance on one House Report regarding a bill that was never formally introduced (Mot. 11), proves nothing. That bill would have rewritten the EFTA to protect consumers "when they are defrauded into initiating a transfer" (H. Rep. 117-701, at 158), which would be a sea change in federal payments law by imposing liability on banks for transactions initiated not by scammers but by consumers themselves. Tellingly, the hearing transcript attached by Citi does not refer to the wire networks until page 86 of 97, and only then as among "other gaps and ambiguities that hamper" the EFTA. (ECF No. 13-9, at 86.) This is "a particularly dangerous ground on which to rest an interpretation of a prior statute." *Central Bank, N.A. v. First Interstate Bank, N.A.*, 511 U.S. 164, 187 (1994). And Citi cites consumer advocates as having urged elimination of the wire exemption (Mot. 11–12), but those advocates specifically described "bank-to-bank wires" as being exempt. (ECF No. 13-11, at 20.)

Citi would like to portray this case as breaking new legal ground, but that is backwards. The reality is that Citi's provision of electronic access to wire network services is a new factual

[1] One did not involve an executed wire transfer at all. *Stepakoff v. IberiaBank Corp.*, 637 F. Supp. 3d 1309, 1311 (S.D. Fla. 2022). And the remainder involved pro se plaintiffs who did not brief the issues. *See Fischer & Mandell LLP v. Citibank, N.A.*, No. 09 Civ. 1160, 2009 WL 1767621, *4 (S.D.N.Y. Jun. 22, 2019) (plaintiff's briefing "declines to address the EFTA claim at all" and "Plaintiff fails to even allege a prima facia violation of the EFTA"); *McClellon v. Bank of Am., N.A.*, No. 18 Civ. 829, 2018 WL 4852628, at *1 & n.1 (W.D. Wash. Oct. 5, 2018) (pro se 3-page complaint was "one of six lawsuits filed . . . against various financial institutions").

development requiring this Court to confront the application of a long-standing set of statutory and regulatory language to a new fact pattern. And guidance exists already: Beneficiary banks have for years had the ability to complete the other side of a wire transfer—their payment obligation—via EFT, and regulators have for decades recognized that when they do so the payments are subject to the EFTA and Reg. E. 12 C.F.R. § 210.25, app. A; 12 C.F.R. § 1005.3(c)(3), Supp. I, Comment 3(c)(3). Now that Citi has provided consumers the means to electronically authorize EFTs on the front-end, these payments, like the back-end payments, are subject to these same laws.

E. The EFTA's Automatic Transfer Exemption Is Inapplicable as It Is Limited to Overdraft and Comparable Authorized Account Maintenance Payments

Citi's "alternative" argument that the automatic transfer exemption also exempts Citi's debits in connection with fraudulent Payment Orders (Mot. 22–23) should be rejected as well.

The EFTA itself exempts only transfers between accounts "for the purpose of covering an overdraft or maintaining an agreed upon minimum balance." 15 U.S.C. § 1693a(7)(D); *see Hamilton-Warwick v. U.S. Bancorp*, No. 15 Civ. 2730, 2016 WL 11491393, at *5 (D. Minn. May 18, 2016) ("The EFTA excludes any automatic transfer for overdraft protection."). In first promulgating Reg. E, the Federal Reserve "decided to defer" action on automatic transfers other than overdraft. 44 Fed. Reg. at 18471. While Reg. E has since been broadened slightly to capture recurring, authorized account maintenance charges akin to overdraft, its official interpretation limits the exemption to "debits or credits to consumer accounts for check charges, stop-payment charges, non-sufficient funds (NSF) charges, overdraft charges, provisional credits, error adjustments, and ***similar items***." 12 C.F.R. § 1005.3, Supp. I, Comment 3(c)(5) (emphasis added). A one-time consumer EFT to pay for a large-dollar Payment Order is not remotely similar.

Moreover, the exemption still requires the act that triggers the automatic transfer to be an authorized act, which is not the case in the transactions that are at issue and alleged in the

Complaint. For example, *Krutchkoff v. Fleet Bank, N.A.*, cited by Citi (Mot. 23), involved an "authorized, automatic intra-financial-institution transfers" under which the consumer agreed that a bank would make monthly minimum payments on his bank-issued credit card from his checking account. 960 F. Supp. 541, 544–45 (D. Conn. 1996). As another district court observed, in this and similar cases, "the customer has specifically agreed to periodic debits from her account." *Patel v. PayPal, Inc.*, No. 05 Civ. 4706, 2006 WL 8447989, at *2 (N.D. Cal. Apr. 10, 2006).

Citi's expansive application of the exemption leads to absurd results. For example, Citi's terms and conditions provide that when paying bills online consumers authorize Citi "to withdraw the necessary funds." (ECF No. 13-15, at F.) Were Citi correct that this withdrawal is merely an exempt automatic transfer triggered by the bill payment request, it could effectively contract around its EFTA obligations using the automatic transfer exemption. *See Patel*, 2006 WL 8447989 at *2 (rejecting "expansive" interpretation of exemption because any "series of events could precede the debit of funds" automatically "by a computer"). And Citi's reading also would put it in violation of the compulsory use rule, which prohibits conditioning "an extension of credit to a consumer on the consumer's repayment by preauthorized." EFTs. 12 C.F.R. § 1005.10(e)(1). When Citi accepts a Payment Order, it extends credit by sending its own money to a beneficiary bank via Bank-to-Bank Wire. *See* UCC Pref. Note (funds transfers "involve the giving of credit by the receiving bank to the customer"). Citi's argument that its subsequent collection of payment for this credit is an automatic transfer puts it squarely in violation of this prohibition.

II. THE COMPLAINT ADEQUATELY ALLEGES THAT CITI ILLEGALLY FAILED TO REIMBURSE UNAUTHORIZED INTRA-BANK TRANSFERS THAT PRECEDED FRAUDULENT WIRE TRANSFERS (COUNT II)

The Complaint alleges that: (i) scammers initiated intra-bank EFTs to consolidate funds into a single account (¶¶ 94, 103, 277–78); (ii) funds were used to pay for Payment Orders in amounts larger than would otherwise have been possible (¶ 277), including specific examples (¶¶

127–28, 155–56, 199, 205, 221, 225); and (iii) Citi did not reimburse consumers for these EFTs (¶¶ 277–79.) This is sufficient to allege violations of EFTA and Reg. E. *See Moore v. JPMorgan Chase Bank, N.A.*, No. 22 Civ. 1849, 2022 WL 16856105, at *1–2 (N.D. Cal. Nov. 10, 2022) (denying motion to dismiss where plaintiffs "allege that without the unauthorized (and unknown) transfer of money from their savings to their checking account there would not have been sufficient monies in the checking account to fund the unauthorized (and unknown) wire transfers").

Citi's assertion that consumers received a benefit from these EFTs is absurd. For one, the Complaint expressly alleges that these EFTs enabled larger fraudulent transactions, which plainly is "a detriment, not a benefit." *Id*. at 2. In Citi's own cases the courts looked to what EFTs were used for—a consumer received the "benefit of reducing her debt," *Aikens v. Portfolio Recover Assocs., LLC*, 716 F. App'x 37, 40 (2d Cir. 2017), and a consumer received a "credit to her MBNA account," *Becker v. Genesis Fin. Servs.*, No. 06 Civ. 5037, 2007 WL 4190473, at *12 (E.D. Wash. Nov. 21, 2007). Here, however, consumers' accounts were wholly depleted with no corresponding benefit. Moreover, that the CFPB treats an "EFT at an ATM [as] an unauthorized transfer if the consumer has been induced by force to initiate the transfer," 12 C.F.R. § 1005.2, Supp. I, Comment 2(m), similarly recognizes that it is necessary to look beyond the mere transfer of cash from an ATM to the consumer and to consider that the cash was then taken by the thief.

The Complaint also pleads facts showing two more ways in which the intra-bank transfers were to consumers' detriment. *First*, it alleges that consolidation reduced the total number of Payment Orders and thus reduced scrutiny of fraudulent transactions. (¶¶ 94, 103, 277–78.) The EFTs thus resulted in decreased security. *See Moore*, 2022 WL 16856105 at *2 (distinguishing *Becker* because "the plaintiff, who was not represented by an attorney, did not allege that the transfer among credit cards allowed for a third party to steal the plaintiff's money"). *Second*, it

alleges that funds were transferred from savings accounts to checking accounts (*e.g.*, ¶¶ 127, 155, 199, 221), which deprived consumers of the benefit of their interest-bearing accounts.

Finally, Citi's contention that the OAG fails to plead facts justifying restitution (Mot. 24) does not require dismissal. The OAG can bring claims based on repeated illegal acts in New York, Exec. Law. § 63(12); while restitution is a remedy, it is not an element. *See State v. Ford Motor Co.*, 74 N.Y.2d 495, 496 (1989) (Section 63(12) permits the OAG to enjoin "repeated illegal or fraudulent acts" and "if granted" a court "may also direct restitution" or damages).

III. THE COMPLAINT ADEQUATELY ALLEGES THAT CITI ILLEGALLY AND REPEATEDLY VIOLATED THE EFTA'S WAIVER PROHIBITION AND ITS REQUIREMENT TO MAKE UNDERSTANDABLE DISCLOSURES (COUNT III)

The EFTA prohibits contracts containing "any provision which constitutes a waiver of any right conferred," 15 U.S.C. § 1693l, and requires disclosures to be "readily understandable," 15 U.S.C. § 1693c(a). The Complaint alleges three violations of these commands.

First, Citi's terms and conditions treat EFTs initiated with usernames and passwords as authorized (¶ 286(a)), limiting consumers' ability to show that EFTs were unauthorized. Citi does not contest this interpretation but argues there is no allegation that Citi relied upon it. (Mot. 25.) That is wrong: The Complaint alleges that certain of Citi's denials were based on consumers "providing . . . authorization for the transactions." (¶¶ 65, 136, 214, 229, 261.) From this it "is reasonable to infer that [Citi] applied the challenged" provision even if it is not "explicitly allege[d]." *Sparkman v. Comerica Bank*, No. 23 Civ. 2028, 2023 WL 8852487, at *6–7 (N.D. Cal. Dec. 21, 2023). Citi also is wrong that such allegations are required. The EFTA provides that no agreement "may contain any provision which constitutes a waiver of any right." 15 U.S.C. § 1693l. This prohibition "does not regulate practice, but content," which is sensible because "nothing precludes [Citi] from changing course" and invoking a prohibited provision later. *Simone v. M&M Fitness LLC*, No. 16 Civ. 1229, 2017 WL 1318012, at *4 (D. Ariz. Apr. 10, 2017).

Second, Citi concedes that the terms and conditions create "an evidentiary presumption" (Mot. 26) that Citi's own records are "conclusive" evidence of any "action taken through" online or mobile banking, absent "substantial" contrary evidence. (¶¶ 54, 89.) This makes it easier for Citi to meet its burden to determine that an error did not occur and deny reimbursement, 15 U.S.C. §§ 1693f(d), 1693g(b), by disregarding or limiting the effect of contrary evidence (¶ 268(b)). For example, Citi denied reimbursement for Consumer G, who suffered a SIM swap (¶ 198) verified by his provider (¶ 206) and Consumer C (¶ 158), who received confirmation that his mortgage provider was hacked (¶ 154). The presumption also relieves Citi of its obligation to undertake a reasonable investigation, 15 U.S.C. § 1693f; 12 C.F.R. § 1005.11, because if Citi's own records of receipt of authorization through online or mobile banking platforms are "conclusive" as to the question of authorization then the scope of what is reasonable is narrower. (¶ 289(c).) For example, the Complaint alleges that Citi frequently did not interview consumers (*e.g.*, ¶¶ 136, 152, 165, 229, 261)—an omission that is defensible only in light of the improper presumption.

Finally, the Complaint alleges that Cit's security procedures (¶ 84) describe in vague and uncertain terms how Citi will verify Payment Orders (¶¶ 87–88, 285). Citi argues that there is no obligation to disclose security procedures. (Mot. 24.) The claim is not premised on Citi's failure to make a required disclosure, however, but on Citi, having chosen to make a disclosure, having done so using insufficiently understandable terms (¶¶ 281–85). Nor must Citi provide a "roadmap" for scammers. (Mot. 24–25). But under the written terms and conditions, a consumer is unable to know with any clarity what efforts Citi ***might*** undertake to verify a large-dollar Payment Orders (¶ 84), or even ***if*** Citi will take any steps beyond the username and password (*e.g.*, ¶ 88). That is not close to the requirement that consumers be able to readily understand their agreements.

IV. THE COMPLAINT ADEQUATELY ALLEGES REPEATED ILLEGALITY BASED ON CITI'S REPEATED FAILURES TO REIMBURSE CONSUMERS FOR FRAUDULENT PAYMENT ORDERS UNDER THE UCC (COUNT IV)

The Complaint alleges the existence of unauthorized and ineffective Payment Orders that Citi did not reimburse in violation of the UCC. (¶¶ 11–13, 288–97.) Citi contends the Payment Orders were effective, U.C.C. § 4A-204(1), which requires both (i) the existence of an agreed-upon security procedure and (ii) Citi to "prove[] that it accepted" the Payment Order "in good faith and in compliance with" the security procedure and any customer instructions, *id*. § 4A-202(2). This latter requirement shifts the burden of proof to Citi. *See Experi-Metal, Inc. v. Comerica Bank*, No. 09 Civ. 14890, 2010 WL 2720914, at *7 (E.D. Mich. Jul. 8, 2010) (bank "has the burden of proving" effectiveness under Article 4A). Count V should be sustained for three reasons:

A. The Single-Factor Authentication Protocol in Citi's Adhesive Online Terms and Conditions Is Commercially Unreasonable as a Matter of Law

Citi's terms and conditions state that it issues "a User ID and Passwords ('Codes')" and "any instruction made on Citi Online with valid Codes" is "authorized" and executed "regardless of the identity" of who sent the instruction. (¶ 84.) Consumers must "confirm" (¶¶ 84–86) that this is "commercially reasonable and appropriate" (¶ 84). The terms also state that Citi "may" employ other tools for verification (¶ 84) at its sole discretion. By the agreement's plain language, the only agreed-upon procedure is the single-factor use of a username and password. *See Sidney Frank Importing Co., Inc. v. Beam Inc.*, 998 F. Supp. 2d 193, 205 (S.D.N.Y. 2014) ("Generally, the term 'may' is not used to convey a mandatory obligation."). For example, in *Chavez v. Mercantil Commercebank, N.A.*, cited by Citi, the Eleventh Circuit looked solely to the one mandatory procedure in the agreement and not to other "means to verify any Payment Order" that the bank "may use" because the discretionary controls the bank "may use" did not "constitute an agreement" with its customer on a specific security procedure. 701 F.3d 896, 897–98 (11th Cir 2012).

Single-factor verification protocols for large-dollar Payment Orders are not commercially reasonable, per leading industry guidance (¶ 71) that Citi does not contest (*see* Mot. 30). Courts also agree. *See Choice Escrow*, 754 F.3d at 620 (single-factor protocols "are inadequate to safeguard against modern Internet fraud"); *Texas Brand Bank v. Luna & Luna, LLP*, No. 14 Civ. 1134, 2015 WL 12916411, at *4 (N.D. Tex. Feb. 27, 2015) ("[I]ndustry standards require security procedures to use more than one level of authentication to be commercially reasonable.").

Citi cites *Braga Filho v. Interaudi Bank* as an example of a "flexible" security procedure (Mot. 28–29), but in that case the security procedure provided that the bank "would select security procedures"—not that it may, No. 03 Civ. 4795, 2008 WL 1752693, at *1 (S.D.N.Y. Apr. 16, 2008). And at summary judgment, the evidence showed that the bank selected a security procedure that was not discretionary at all but "***required***" both a "***mandatory*** signature comparison" and three more steps: faxes "***had to be*** confirmed by telephone call"; the sender "***had to answer*** security questions"; and the call "***had to be*** logged and recorded." *Id*. at *4 (emphasis added).

Citi's claim that the Complaint lacks "allegations about what procedures were employed or why they were lacking" (Mot. 30), is also meritless. For one, it is false: the Complaint alleges consumers—including Consumer A (¶¶ 123–38), Consumer C (¶¶ 153–58), Consumer E (¶¶ 168–81), and Consumer I (¶¶ 232–47)—had large-dollar Payment Orders accepted without further contact, from which the Court can infer reliance on single-factor protocols. This argument also "confuses" the burden of proof, as it is Citi who is obligated to prove what procedure was followed. *See Burge v. JPMorgan Chase Bank, N.A.*, No. 22 Civ. 607, 2023 WL 3778276, at *3 (S.D. Ind. Mar. 28, 2023) (complaint's failure to "identif[y] the security procedure" used "does not prove that [the bank] in fact employed a commercially reasonable security procedure"). Citi will have an opportunity to prove up its procedures later; that is no basis for dismissal at this stage.

B. The Complaint Alleges Facts Giving Rise to Reasonable Inferences that Citi's Security Procedure Was Not Commercially Reasonable

Even were Citi's discretionary protocols relevant, the Complaint alleges facts from which to infer unreasonableness. Article 4A requires that a commercially reasonable security procedure account for "the circumstances of the customer known to the bank." U.C.C. § 4A-202(2); *see Centre-Point Merchant Bank Ltd. v. Am. Express Bank Ltd.*, No. 95 Civ. 5000, 2000 WL 1772874, at *4–5 (S.D.N.Y. Nov. 30, 2000) (test is "whether the procedure is reasonable for the particular customer and the particular bank" given "the circumstances of the customer known to the bank"). This is not some "toehold for regulating through litigation" (Mot. 32) nor does the Complaint urge the sort of "transactional analysis" (Mot. 31) in which "a human being manually reviews every payment order submitted to the bank to ensure that no irregularities exist," which the Eight Circuit rejected as necessary in an otherwise inapposite commercial case. *Choice Escrow*, 754 F.3d at 614, 618–19. What is required, however, is that the Court "consider" the circumstances of the customer "in determining if [Citi]'s security procedure is commercially reasonable." *Id*. at 619.

The Complaint alleges that Citi's security procedure did not account for consumers. For one, as it does not contest (*see* Mot. 27–33), Citi employs a single, predetermined, non-negotiable security procedure for all consumer accounts (¶¶ 84–86). Applying an identical security procedure to an entire class of consumer customers, regardless of account balance, transaction history, or other factors known to Citi, is not commercially reasonable. *See Patco Constr. Co., Inc. v. People's United Bank*, 684 F.3d 197, 212 (1st Cir. 2012) (security procedure with verification protocols that adhered to a "one-size-fits-all" approach was commercially unreasonable).

Citi's suggestion that the Complaint alleges "antifraud practices that . . . are inadequate" but not "multiple, particular instances" of UCC violations (Mot. 27) also is meritless. The Complaint specifically alleges multiple instances in which Citi was aware of anomalous account

activity but which, in the face of such activity, Citi "failed to materially alter and employ its most robust verification procedures." (¶ 293(b).) Examples of these failures include:

- Citi's procedures do not trigger enhanced verification of Payment Orders that were the first ever or would empty accounts (¶¶ 105–06), as reflected in at least the experiences of Consumer A (¶¶ 123–38), Consumer C (¶¶ 153–58), Consumer E (¶¶ 168–81), and Consumer I (¶¶ 232–47).

- Citi's procedures do not trigger enhanced verification of Payment Orders following suspicious activity calling into question whether the consumer is involved, such as consolidation of funds into a single account before wiring out everything (¶ 103), as reflected in at least the experiences of Consumer C (¶¶ 153–58), Consumer G (¶¶ 197–216), and Consumer H (¶¶ 217–31).

- Citi's procedures do not trigger enhanced verification of Payment Orders submitted after anomalous activity suggesting compromise, such as changes to usernames and passwords or updates to account status (¶ 101–02), as reflected in at least the experiences of Consumer A (¶¶ 123–38), Consumer B (¶¶ 139–52), Consumer D (¶¶ 159–67), and Consumer J (¶¶ 248–62).

- Citi's procedures do not trigger enhanced verification of Payment Orders after Citi attempted but failed direct contact verification (¶ 104), as reflected in at least the experiences of Consumer A (¶¶ 123–38), Consumer G (¶¶ 197–216), Consumer H (¶¶ 217–31), and Consumer J (¶¶ 248–62).

These allegations establish that Citi's security procedure did not trigger robust verification of out-of-the-ordinary activity and thus failed to account for "the circumstances of the customer as known to the bank." It thus was not commercially reasonable. *Rodriguez v. Branch Banking & Trust Co.*, 46 F.4th 1247, 1259 (11th Cir. 2022). Nothing more is required at this stage. *Cf. 800 Columbia Project Co. LLC v. CMB Wing Lung Bank Ltd.*, No. 21 Civ. 278, 2022 WL 17884221, at *13 (C.D. Cal. Sep. 19, 2022) (expert testimony on "industry standards will be particularly instructive for the Court's assessment of whether such a security procedure is commercially reasonable").

C. The Complaint Adequately Alleges Facts Showing that Citi Did Not Follow Security Procedures, Did Not Act in Good Faith, and Did Not Act in a Manner Consistent with Contrary Consumer Instructions

The Complaint's detailed allegations of multiple consumer experiences, which Citi simply ignores, provide more than sufficient facts from which the Court can infer that Citi has not proven

that Payment Orders were effective. On this issue, Citi bears the burden to prove its good faith acceptance of Payment Orders, as well as its compliance with security procedures and consumer instructions. U.C.C. § 4A-202(2). Thus, the OAG's "obligation to produce evidence at the motion to dismiss stage is even further reduced" at this stage. *Ellington Long Term Fund, Ltd. v. Goldman Sachs & Co.*, No. 09 Civ. 9802, 2010 WL 1838730, at *4 (S.D.N.Y. May 4, 2010).

First, multiple consumers did not share account or security information and Citi did not make contact with the consumers before large-dollar Payment Orders were accepted, (*see* ¶¶ 123–38 (Consumer A); ¶¶ 168–81 (Consumer E); ¶¶ 217–31 (Consumer H))—facts from which it is reasonable to infer that Citi did not adhere to its security procedures at all.

Second, the Complaint pleads facts sufficient to infer a lack good faith, which is more than "technical compliance with a security procedure" but requires Citi to act "in a way that reflects the parties' reasonable expectations." *Choice Escrow*, 754 F.3d at 623. For example:

- Citi accepted fraudulent Payment Orders on at least two occasions ***after*** it had placed automated phone calls to consumers who responded by clicking buttons stating that the activity was unauthorized (¶¶ 139–44, 182–87);
- Citi accepted a fraudulent Payment Order from a consumer's checking account shortly ***after*** it had rejected prior Payment Orders and locked his savings accounts following a suspicious caller referral (¶¶ 199–205); and
- Citi accepted two fraudulent Payment Orders ***after*** a consumer had called into Citi's customer service number and described her recent interactions with a scammer that day before to a Citi representative (¶¶ 253–57).

These facts plainly show a lack of good faith. *E.g.*, *Essgeekay Corp. v. TD Bank, N.A.*, No. 18 Civ. 3663, 2018 WL 6716830, at *4 (D.N.J. Dec. 19, 2018) (lack of good faith where bank accepted Payment Orders "*despite* suspicions that they were fraudulent") (emphasis in original).

Third, multiple consumers never personally enrolled in online wire transfer services and thus had not authorized Citi to accept ***any*** electronically initiated Payment Orders, yet Citi accepted several fraudulent Payment Orders. (¶¶ 92, 126–28, 145–46, 171–72, 199–202.)

Finally, multiple consumers spoke directly with Citi representatives and told them to reject pending Payment Orders, but instead Citi accepted the Payment Orders in contravention of these clear instructions. (*See* ¶¶ 161–63 (Consumer D); ¶¶ 238–40 (Consumer I).)

D. The Complaint Also Alleges – and Citi Does Not Contest – a Failure to Pay Statutorily Required Interest When Reimbursing under Article 4A

Article 4A of the UCC requires Citi to pay "interest on the refundable amount" when reimbursing consumers for unauthorized and ineffective Payment Orders. U.C.C. § 4A-204(1). The Complaint alleges that Citi does not always do so (¶¶ 119, 296), and alleges specific examples of such failures (¶¶ 247, 262). Citi offers no response, and this claim should be sustained.

V. THE COMPLAINT ADEQUATELY ALLEGES THAT CITI ILLEGALLY FAILED TO PROTECT CONSUMER FINANCIAL INFORMATION OR RESPOND APPROPRIATELY TO RED FLAGS (COUNTS V & VI)

The Complaint alleges substantial facts as to shortcomings in Citi's data security practices and procedures in violation of New York's SHIELD Act (Count V) and Red Flag Rule (Count VI). The motion to dismiss these claims ignores these allegations and should be denied.

A. The Complaint Alleges Facts Sufficient to Infer that Citi Failed to Protect Consumer Financial Information in Violation of New York's SHIELD Act

New York's SHIELD Act requires Citi to develop and maintain reasonable safeguards to protect financial account information, including technical safeguards to detect and respond to system attacks or failures, GBL § 899-bb(2)(b)(ii)(B)(3), and administrative safeguards to train employees in the security program, *id*. § 899-bb(2)(b)(ii)(A)(2)–(4). This is not merely an anti-hacking and notification statute (Mot. 39), as New York has a separate law to that effect. *See* GBL § 899-aa; *see also* N.Y. Bill Jacket L. 2019, Ch. 117, at 7 (through SHIELD Act New York joins "the increasing number of states that require reasonable data security protections"). The SHIELD Act requires Citi to protect "integrity" of confidential financial account information, GBL § 899-

bb(2)(a), to address "external" threats to its systems, *id*. § 899-bb(2)(b)(ii)(A)(2), and to assess risks in information "transmission," *id*. § 899-bb(2)(b)(ii)(B)(2).

The Complaint alleges facts showing that Citi failed to satisfy these obligations. (¶¶ 303–05.) Consumers had accounts infiltrated without ever speaking with, or providing information, to scammers directly. (*E.g.*, ¶¶ 124, 169, 198.) Specific, repeat scams that targeted Citi's systemic vulnerabilities went unaddressed for years. (¶¶ 29–32, 140, 170–72, 199–205, 236, 249.) And Citi employees were poorly trained and responded inadequately to potential security breaches: front-line representatives were not trained or empowered to effectively secure accounts (*e.g.*, ¶¶ 110–13, 125); those representatives frequently placed consumers on lengthy holds while scammers remained able to access online or mobile banking (*e.g.*, ¶¶ 108–09, 239–40); and Citi employees misstated the security of consumer financial information (*e.g.*, ¶¶ 7, 115, 209, 254).

These allegations do not simply rely on isolated breaches of confidential information, as Citi suggests. (Mot. 40.) In *FTC v. Wyndham Worldwide Corp.*, the district court sustained claims where the FTC did not "simply assert that a violation" of data security laws "must have occurred simply because" it had alleged that data breaches occurred; instead, the FTC alleged "several data-security insufficiencies" such as "failing to employ firewalls," employing "commonly-known default user IDs and passwords," and "failing to restrict third-party access" to data systems. 10 F. Supp. 3d 602, 625–26 (D.N.J. 2014). Here, too, the Complaint's allegations of Citi's failure to respond to known gaps in security and adequately train personnel are "insufficiencies that, drawing reasonable inferences in favor" of the OAG, "led to" violations of law. *Id*. at 626; *see Toretto v. Donnelly Fin. Solutions, Inc.*, 583 F. Supp. 3d 570, 595 (S.D.N.Y. 2022) (allegations that defendant "failed to implement [sufficient] security systems," had "deficient controls," and was aware "that it was a target of cybersecurity threats" sufficient to allege breach of duty).

B. The Complaint Alleges Facts Sufficient to Infer that Citi Failed to Develop and Implement Protocols Designed to Respond Appropriately to Red Flags

The Red Flag Rule requires Citi to implement "programs to protect consumers from identity theft." *ABA v. FTC*, 636 F.3d 641, 643 (D.C. Cir. 2011); 16 C.F.R. § 681.1(d)(2)(ii). Appropriate bank security programs must evaluate "aggravating factors that may heighten the risk of identity theft in determining an appropriate response to" red flags. 72 Fed. Reg. 63718, 63723 (Nov. 9, 2007). And when responding to such red flags, banks must respond appropriately to "prevent and mitigate" harm. 16 C.F.R. § 681.1(d)(2)(iii). By contrast, where banks do not take further action to prevent and mitigate harm, they must "have a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft." 72 Fed. Reg. at 63729.

The Complaint alleges in detail that Citi did not have policies in place to effectively identify anomalous activity by scammers as potential identity theft or to mitigate resulting harms. (¶ 315.) Obvious red flags were not treated as such, including consolidations of consumers' funds into a single account (*e.g.*, ¶¶ 62, 94, 103), attempted Payment Orders submitted shortly after failed ones (*e.g.*, ¶¶ 104, 144, 203, 225), or changes to account status or enrollment in wire transfer services (*e.g.*, ¶¶ 92, 102, 126, 146, 199). Citi also did not treat the ultimate red flag of an unprecedented, large-dollar Payment Order as such. *See Burge*, 2023 WL 3778276 at *4 (wire transfers amounting to tens of thousands of dollars sent from accounts that "did not have *any* history of wire transfers" can fairly be called "red flags"). Nor did Citi's policies reasonably mitigate harm following red flags; for example, while Citi required representatives to lock accounts and require in-person verification in response to notices of fraudulent payment activity (¶ 59), a similar requirement is not in place to mitigate harm when Citi detects red flags suggesting identity theft (¶ 315).

Contrary to Citi's contention (Mot. 38), this lawsuit is not an effort to impose "strict liability," but a response to specific, identified flaws in Citi's policies and procedures. It thus stands

in stark contrast to the cases cited in Citi's motion to dismiss. *See, e.g.*, *Mastin v. Ditech Fin., LLC*, No. 17 Civ. 368, 2018 WL 524871, at *6 (E.D. Va. Jan. 23, 2018) (complaint contained no allegations whatsoever that the defendant "failed to maintain policies and procedures that are reasonably designed to achieve" required regulatory objectives).[2]

C. The OAG's SHIELD Act and Red Flag Rule Claims Are Not Preempted

Citi argues that Counts V and VI are preempted by the Fair Credit Reporting Act ("FCRA") (Mot. 34–36, 41), which provides that states may enact no "requirement or prohibition" with "respect to the conduct required" by the Red Flag Rule. 15 U.S.C. § 1681t(b)(5)(F). Not so.

In assessing preemption, courts start with the presumption that "federal statutes do not preempt state law," particularly in traditional areas of state regulation such as consumer protection, and "ordinarily accept the reading that disfavors pre-emption." *Galper v. JPMorgan Chase Bank, N.A.*, 802 F.3d 437, 448 (2d Cir. 2015). Here, the CFPB has advised that the FCRA's preemption provisions "have a narrow and targeted scope" and that states "retain substantial flexibility to pass laws" that "reflect emerging problems." 87 Fed. Reg. 41042, 41042 (Jul. 11, 2022). Discussing Section 1681t(b)(5) in particular, the CFPB explained that the "term 'with respect to' indicates that Congress intended these provisions to have a narrow sweep." *Id*. at 41043. Thus, the FCRA prohibits state laws imposing requirements that ***differ*** from federal ones; for example, the FCRA requires that annual credit reports be provided, and a state law that requires "semi-annual credit reports" would likely be preempted, while a state law requiring that reports provide information "in languages other than English" would likely not be preempted. *Id*. at 41046; *see Willey v. J. P.*

---

[2] *See Hines v. Regional Bank*, No. 16 Civ. 1996, 2018 WL 905364, at *5 (N.D. Ala. Feb. 15, 2018) (complaint did "not allege [defendant] failed to implement policies reasonably designed to achieve that section's objectives"); *Smith v. Franklin/Templeton Distribs., Inc.*, No. 09 Civ. 4775, 2010 WL 4286326, at *3 (N.D. Cal. Oct. 22, 2010) ("[P]laintiff has failed to allege facts showing that the fund or funds at issue failed to adopt and implement compliance programs"); *see also Mikel v. Carrington Mortg. Services, LLC*, No. 16 Civ. 1107, 2019 WL 4060890, at *7 (W.D. Tex. Jun. 25, 2019) (plaintiff presented "no evidence regarding . . . policies and procedures").

Morgan Chase, N.A., No. 09 Civ. 1397, 2009 WL 1938987, at *8 (S.D.N.Y. Jul. 7, 2009) ("with respect to" prong of Section 1681t(b)(5) is "narrower"). The Second Circuit, interpreting a parallel FCRA provision, also held that the phrase "with respect to" means state law is preempted only when it "concerns th[e] subject matter" covered by federal law. *Galper*, 802 F.3d at 445.

The SHIELD Act plainly is not preempted under these guiding principles, as it concerns Citi's illegal failures to safeguard consumer financial information (*e.g.*, ¶ 305) and to adequately train its employees to effectively secure such information (*e.g.*, ¶ 304), which are wholly distinct from the Red Flag Rule's requirements for identification of potential identity theft and mitigation of related harm (*e.g.*, ¶ 315). This case stands in contrast to those cited by Citi, in which the FCRA preempted state laws concerning the ***exact same conduct***. *See Willey*, 2009 WL 1938987 at *8 (FCRA guidelines for "safeguarding and disposal of consumer information" and "requirements for giving consumers notice" preempt state claims for failure "to safeguard consumer data and [failure] to notify consumers of the data loss"); *see also Elias v. Synchrony Bank*, No. BC555883, 2016 WL 6270746, at *10 (Cal. Super. Ct. Oct. 25, 2016) (invasion of privacy claim preempted by FCRA where premised on "Defendant's failure to recognize . . . red flags"). And to the extent any overlap does exist, preemption should be limited solely to any overlap. *See Noffsinger v. SSC Niantic Operating Co. LLC*, 273 F. Supp. 3d 326, 334 (D. Conn. 2017) ("in preemption cases" a "federal court should not extend its invalidation of a statute further than necessary").

With respect to Count VI, the argument for preemption is nonsensical as the OAG is simply ***enforcing the Red Flag Rule***. Executive Law § 63(12) is a regulatory tool that, among other things, gives the OAG "standing to redress liabilities recognized elsewhere in the law." *People v. Credit Suisse Secs. (USA) LLC*, 31 N.Y.3d 622, 633 (2018). Its "plain language" encompasses all forms of illegality, such as "violations of state or federal law," *James v. Scores*, 79 Misc. 3d 1118, 1122–

23 (N.Y. Sup. Ct. 2023), even where states have no independent enforcement authority, *State v. UPS*, 160 F. Supp. 3d 629, 652 (S.D.N.Y. 2016). For example, the OAG has enforced violations of the FTC Act, even though it does not expressly grant such authority. *People v. JUUL Labs, Inc.*, Index No. 452168-2019, 2022 WL 2757512, at *8–9 (N.Y. Sup. Ct. Jul. 14, 2022); *see also People v. World Interactive Gaming Corp.*, 185 Misc. 2d 852, 861 (N.Y. Sup. Ct. 1999).

Nor does the OAG's Red Flag Rule enforcement run afoul of Congress's stated goal of uniformity, which it sought to achieve by preempting "state and local governments from enacting ***laws that are different from the FCRA***." H.R. Rep. 108-263; *see* H.R. Conf. Rep. 108-396 (legislation creates "a number of ***preemptive national standards***.") (emphasis added throughout).) Executive Law § 63(12) states no "requirements" regarding banks' implementation of procedures for red flags, nor does it "prohibit" any specific conduct. Instead, as Citi acknowledges, it is a "mechanism" to show that relief is appropriate for violations of other laws. (Mot. 27.) This is wholly distinct from Citi's cited cases (Mot. 36, n.13) where private litigants sought to transform substantive state prohibitions with their own elements and scope, such as those barring deception, unfair competition, or unfair trade, into prohibitions on FCRA-covered conduct. *E.g.*, *Manes v. JPMorgan Chase Bank, N.A.*, No. 20 Civ. 11059, 2022 WL 671631, at *5 (S.D.N.Y. Mar. 7, 2022) (state claims for deception and negligence premised on "violations of FCRA").

VI. THE COMPLAINT ADEQUATELY ALLEGES THAT CITI ENGAGED IN FRAUDULENT AND DECEPTIVE CONDUCT (COUNTS VII & VIII)

The OAG is empowered by Executive Law § 63(12) to seek redress for conduct that "has the capacity or tendency to deceive, or creates an atmosphere conducive to fraud," *People v. Gen. Elec. Co.*, 302 A.D.2d 314, 314 (N.Y. App. Div. 2003), while GBL § 349 prohibits conduct that is capable of deceiving a reasonable person, *Gaidon v. Guardian Life Ins. Co.*, 94 N.Y.2d 330, 348 (1999). These laws protect "not only the average consumer, but also the ignorant, the unthinking,

and the credulous." *Gen. Elec.*, 302 A.D.2d at 314. Contrary to Citi's assertion (Mot. 42–45), the "Attorney General may" seek relief under GBL § 349 "without a showing of injury." *Goshen v. Mut. Life Ins. Co.*, 98 N.Y.2d 314, 324 (2002) (contrasting § 349(b), which authorizes OAG action, with § 349(h), which provides a private cause of action to "any person ***who has been injured by reason*** of any violation") (emphasis added).[3] Nor do these statutes require the OAG to establish the common law fraud elements of intent to deceive or reliance. *People v. Trump Entrepreneur Initiative LLC*, 137 A.D.3d 409, 417 (N.Y. App. Div. 2016); *Koch v. Acker, Merrall & Condit Co.*, 18 N.Y.3d 940 (2012). The Complaint states multiple bases for relief under these laws:

Deceptive EFTA Claim Handling. Under the EFTA, Citi cannot condition its obligations to investigate errors on a particular form of notice and must provisionally credit accounts, yet the Citi regularly told consumers no investigation would begin until an affidavit was completed (¶¶ 8, 15, 60, 118, 132, 151, 164), and Citi never credited consumer accounts (¶¶ 62, 120), thereby deceiving consumers (¶¶ 319(b), 324(b).) The Complaint also alleges that Citi's letter-denials falsely assert that consumers' sharing of account or security information with scammers is relevant (¶¶ 319(h), 324(h)), when it is not. *See Green v. Capital One, N.A.*, 557 F. Supp. 3d 441, 448 (S.D.N.Y. 2021) (holding "that access to account information that was furnished in the first instance under fraudulent pretenses is not 'authorized' access under the EFTA").

Deceptive UCC Claim Handling. Under the UCC, Citi cannot deny reimbursement unless it can "prove" that the Payment Order was still effective, which requires Citi to "prove" that the breach of security procedures was the fault of its customers and not Citi. U.C.C. § 4A-202(2). Here, the Complaint alleges that Citi extracted sworn evidence of purported negligence (¶¶ 9, 61,

[3] To the extent *People v. Applied Card Sys., Inc.*, 27 A.D.3d 104, 106 (N.Y. App. Div. 2005), cited by Citi (Mot. 42), suggests otherwise, it is contrary to the Court of Appeals' *Goshen* ruling and is not an authoritative statement of New York law. Tellingly, the *Applied Card* Court cited *Small v. Lorillard Tobacco Co.*, in which the Court of Appeals cited GBL § 349(h) to describe a private litigant's claim as "legally flawed." 94 N.Y.2d 43, 56 (1999).

63), which Citi used to satisfy its own UCC burdens and blame consumers (¶¶ 61, 64–65), under the guise of telling consumers the sworn affidavits were necessary to facilitate Citi's investigation and recovery of stolen funds (¶¶ 8, 15, 60, 118, 132, 151, 164). In *CFPB v. Navient Corp.*, the complaint adequately alleged that a practice of telling consumers that providing incomplete or inaccurate information would result in processing delays was deceptive when doing so "could have several irreversible consequences" because a "fair inference" is that borrowers were "not as careful when filling out the form as they would have been if they had known the true consequences." No. 17 Civ. 101, 2017 WL 3380530, at *23–24 (M.D. Pa. Aug. 4, 2017). Here, it is fair inference that borrowers would not have handed over sworn evidence had they known that Citi would use it against them. In contrast, *Cline v. TouchTunes Music Corp.*, cited by Citi (Mot. 44), involved no deception, since there the company declined to provide refunds when its "Terms of Use state that refunds will not be issued," 211 F. Supp. 3d 628, 635–36 (S.D.N.Y. 2016).

Representative Misstatements. The Complaint also alleges that Citi representatives repeatedly made false statements such as that accounts were secure when they were not (¶¶ 319(c), 324(c)) and that consumers would receive their money back when Citi intended to deny claims and delayed recalling funds (¶¶ 319(g), 324(g)). The Complaint contains specific examples of this conduct. (*e.g.*, ¶¶ 124–25 (representative told Consumer A not to worry after describing a phishing attack); ¶ 161 (representative told Consumer D that funds were secured); ¶ 210 (representative told Consumer G he'd receive a refund because the transactions were "fraud").) These are valid bases upon which to sustain these claims, *e.g.*, *People v. N. Leasing Sys., Inc.*, 169 A.D.3d 527, 528–529 (N.Y. App. Div. 2019), and Citi offers no argument whatsoever to the contrary.

Online & Mobile Banking Enrollment. The Complaint alleges that Citi induced consumers to enroll in electronic banking through promises of safety and security while doing so made their

accounts more, and not less, vulnerable to scammers. (¶¶ 319(a), 324(a).) Citi argues that its statements are puffery, but unlike cases involving securities investors or California law (*see* Mot. 42–43), in New York whether a statement is capable of deceiving a reasonable consumer often involves "a question of fact" inappropriate for early resolution. *Kacocha v. Nestle Purina Petcare Co.*, No. 15 Civ. 5489, 2016 WL 4367991, at *14–16 (S.D.N.Y. Aug. 12, 2016); *e.g. Colangelo v. Champion Petfoods USA, Inc.*, No. 18 Civ. 1228, 2020 WL 777462, at *8 (S.D.N.Y. Feb. 18, 2020) (statements dog food was "guaranteed to keep your dog healthy, happy, and strong" was "not so obviously puffing that their significance should be determined as a matter of law").

For these reasons, courts deny dismissal in consumer cases where the deceptive acts could "reasonably influence" consumers or "shape their expectations." *Avola v. Louisiana-Pac. Corp.*. 991 F. Supp. 2d 381, 393–94 (E.D.N.Y. 2013) (collecting cases). Here, the Complaint alleges that Citi promises safety and security when enrolling in online and mobile banking (¶¶ 11, 82–83), while in doing so it in fact enrolls consumers in accounts with less security (¶¶ 77–78, 84, 87), a fact which its enrollment process obscures (¶¶ 85–86.) These increased vulnerabilities are the sort of "objective, measurable" benchmarks that typical puffery lacks. *See Elkind v. Revlon Consumer Prods. Corp.*, No. 14 Civ. 2484, 2015 WL 2344134, at *13 (E.D.N.Y. May 14, 2015) (denying dismissal based on statement that product was "age defying with DNA advantage").

CONCLUSION

For the foregoing reasons, Plaintiff respectfully submits that Counts I through VIII should be sustained in their entirety and Citi's motion to dismiss should be denied.

Dated: May 17, 2024

Respectfully submitted,

LETITIA JAMES
Attorney General of the State of New York

By: */s/ Christopher L. Filburn*
Christopher L. Filburn
Assistant Attorney General
Bureau of Consumer Frauds & Protection
28 Liberty Street, 20th Floor
New York, New York 10005
Tel.: 212.416.8303
Email: christopher.filburn@ag.ny.gov

Of counsel:

Jane M. Azia
Bureau Chief

Laura J. Levine
Deputy Bureau Chief